



QUALYS SECURITY CONFERENCE 2019

# Securing the Digital Transformation with DevOps

Cloud & Container Security Automation

**Badri Raghunathan**

Director of Product Management, Qualys, Inc.

# Agenda

Digital Transformation in 2019

Accelerate DevOps with Qualys Security Platform

- Recent cloud, container security product updates

The road ahead

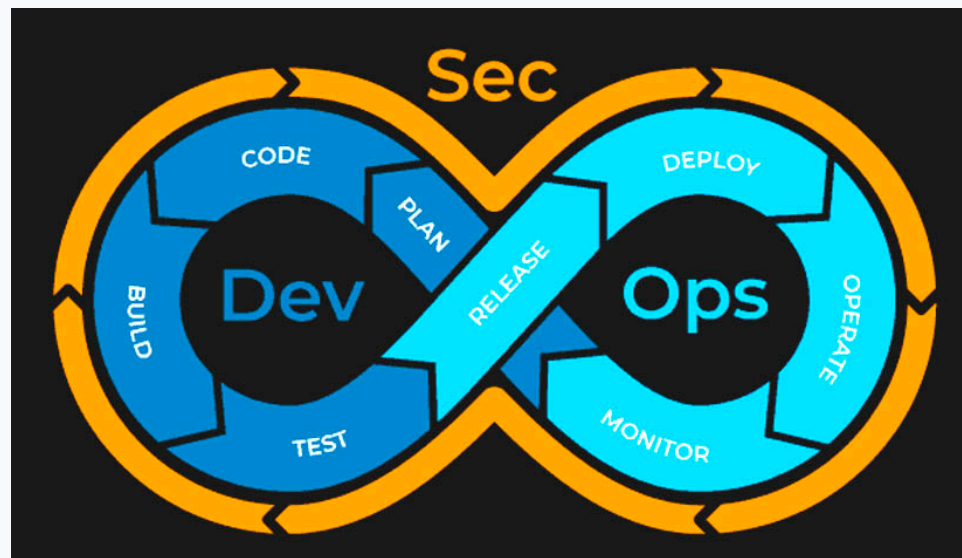
Qualys value proposition for cloud & container security



# Digital Transformation

# The Changing Role of Security

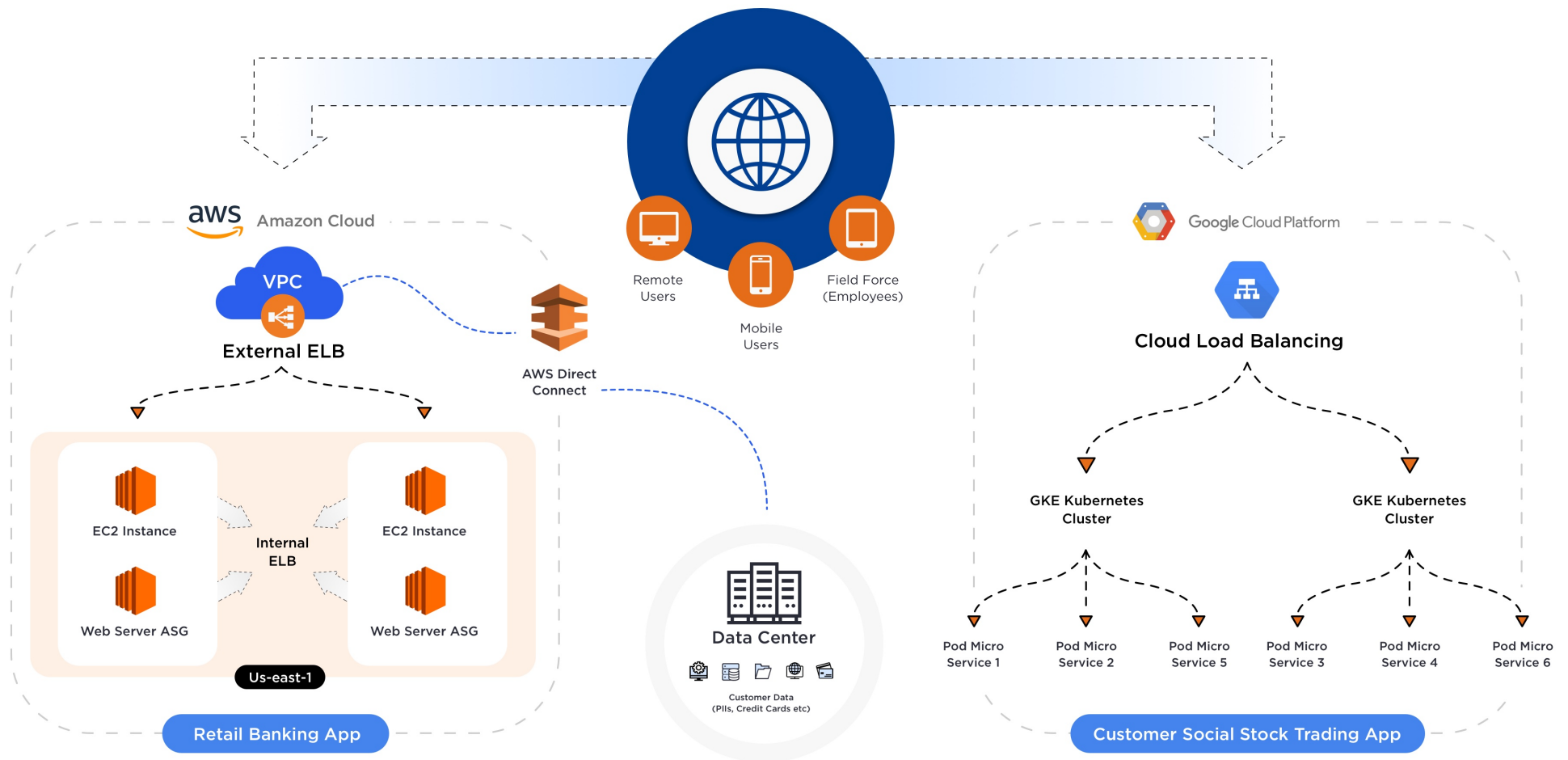
Security selects,  
builds the  
security tooling



DevOps  
operationalizes,  
uses the  
security tooling



## Example Customer Scenario



# Security Challenges in the Cloud

Lack of visibility or control on cloud resources

- Instances, containers, serverless

Misconfiguration of cloud services

Multi cloud environment magnifies security challenges

Lack of a unified toolset for implementing security controls for on-prem & cloud workloads

# Securing Your Cloud Deployments

IaaS	PaaS	SaaS
EC2 Instance, Azure VM, GCP Instance	RDS, Azure SQL Database, Elastic Beanstalk, Containers	Google Suite, Office 365
Cloud Infrastructure S3 Bucket, Security Group, Network Security Group, Storage Blobs, Load Balancers, Firewall Rules		

# Cloud Security

The background is a solid blue rectangle. It is decorated with a grid of small white dots. The dots are arranged in a pattern that is denser at the corners and fades towards the center. There are three prominent red dots: one in the top-left corner, one in the bottom-right corner, and one in the middle-right area.

# Securing Cloud Workloads

## Hardening and Standardizing

### VULNERABILITY MANAGEMENT

- Vulnerability Management (Internal & Perimeter)
- Threat Protection
- Indicators of Compromise
- Patch Management

### POLICY COMPLIANCE

- Policy Compliance (incl. Secure Configuration Assessment)
- File Integrity Monitoring


### APPLICATION SECURITY

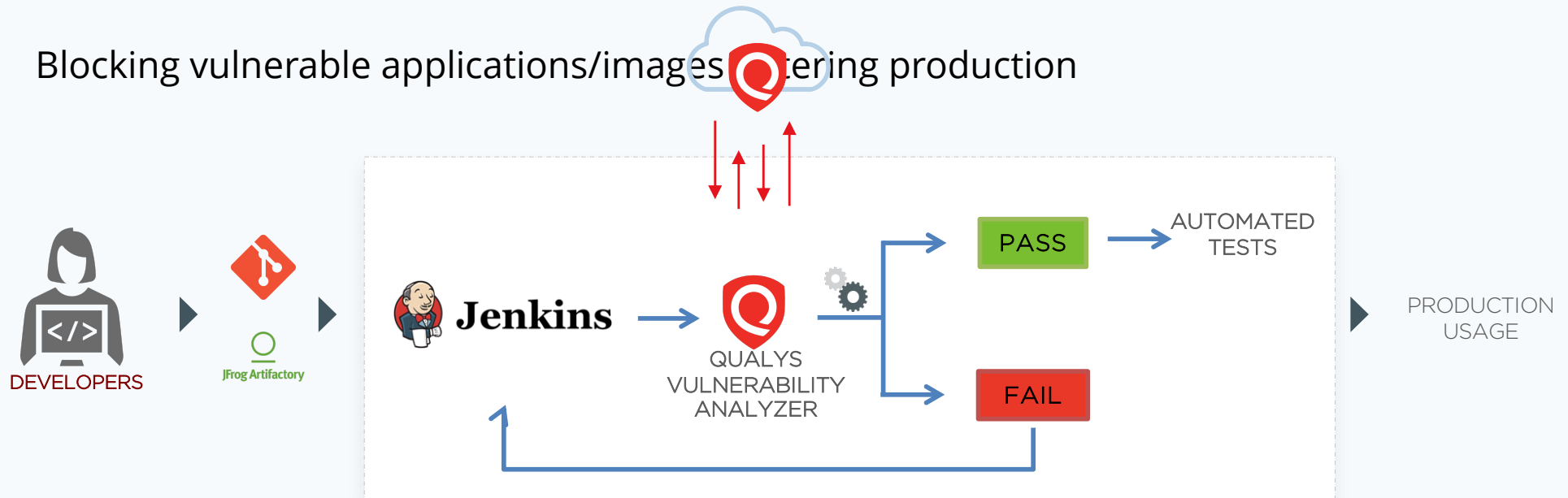
- Web Application Scanning (WebApps and REST APIs)
- Web Application Firewall
- API Security\*

\* Upcoming feature



# Vulnerability Analysis in CI/CD

Blocking vulnerable applications/images  entering production



Supports evaluating – IPs/Hosts, Cloud Instances, and Web Applications

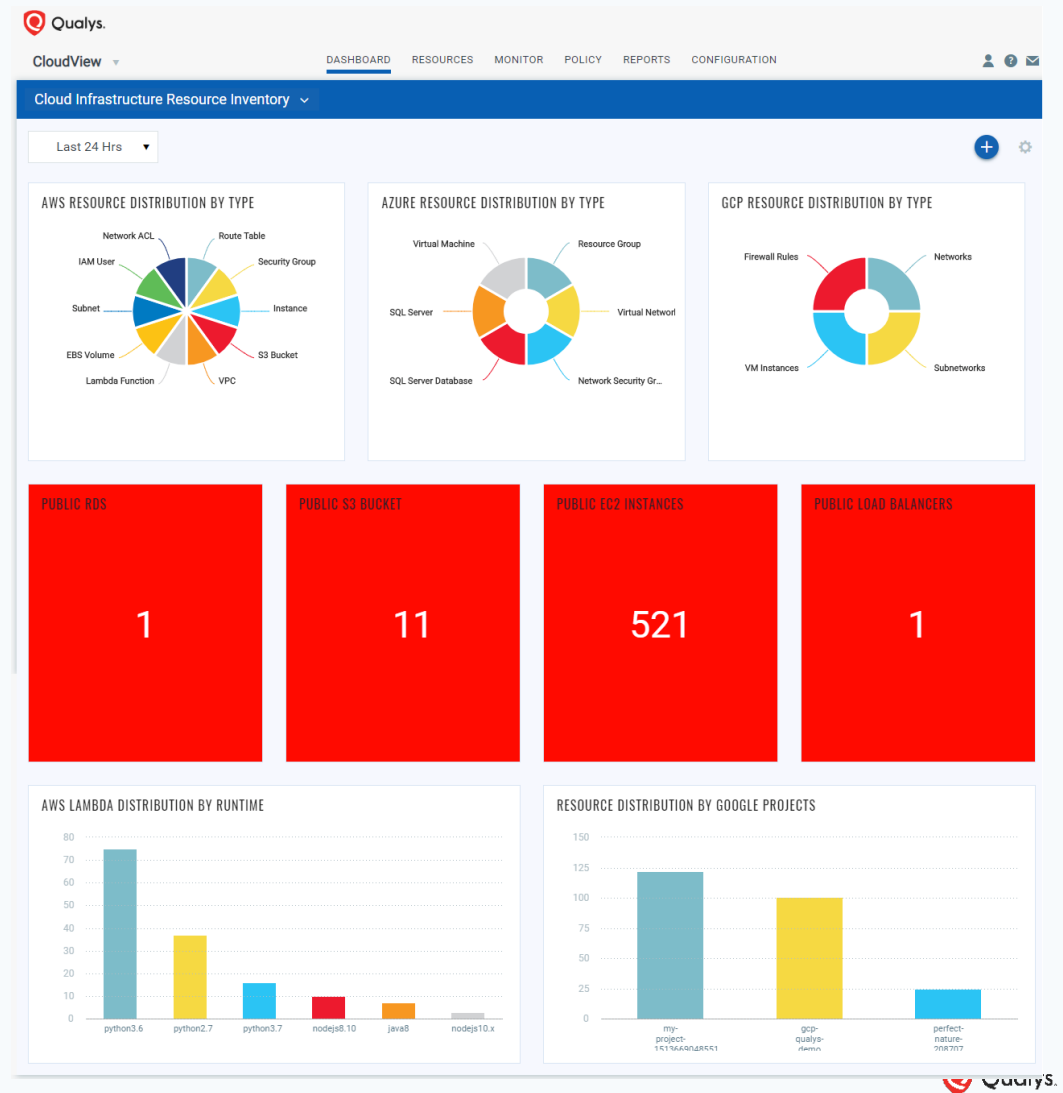
# Rich Visibility with CloudView

Visibility into your cloud resources

Identify public facing/perimeter resources

Resource usage by regions/accounts.

View associations to identify the blast radius

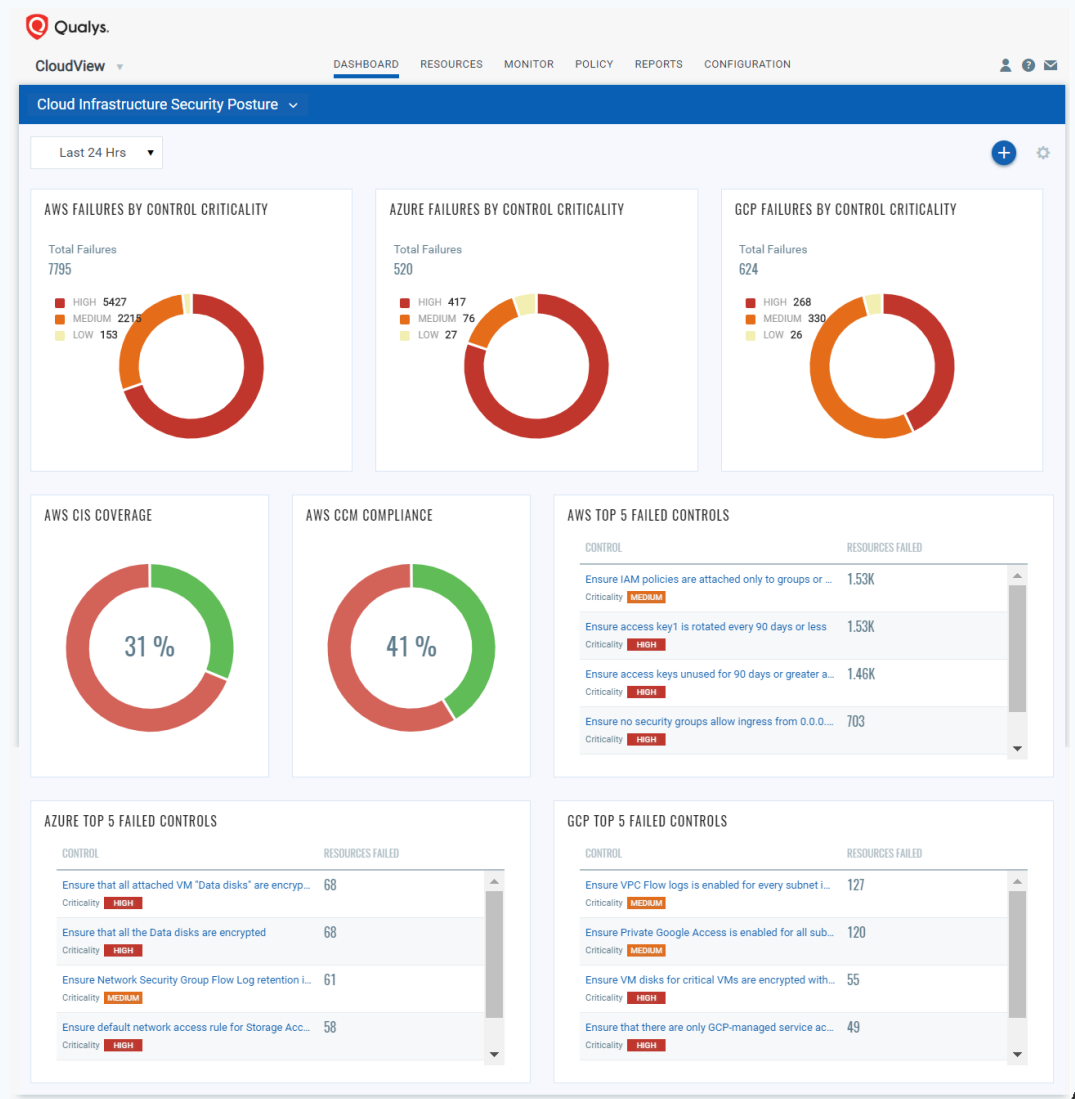


# Compliance Assessment

Identify misconfigured resources

Detect resources that are non-compliant against standards such as CIS Benchmark

Identify top failed controls/account for prioritizing the remediation efforts



# Correlate with Vulnerability Data

Identify vulnerable instances with public IP and associated with the misconfigured security groups

Use vulnerability information for cloud instances to prioritize threats better

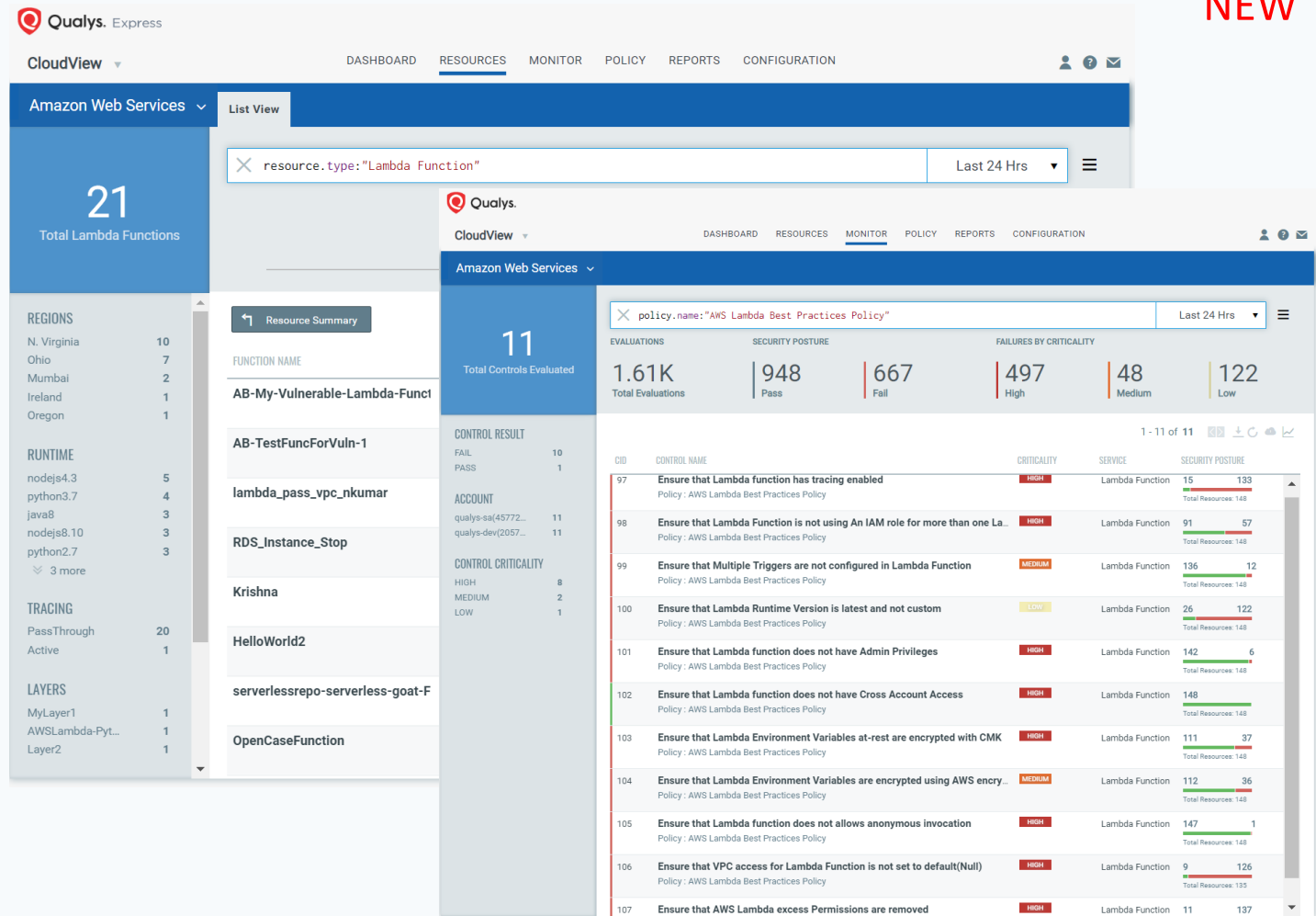
The screenshot displays the Qualys Enterprise CloudView interface. The top navigation bar includes 'DASHBOARD', 'RESOURCES', 'MONITOR', 'POLICY', 'REPORTS', and 'CONFIGURATION'. The left sidebar shows 'Amazon Web Services' with a dropdown menu and a summary of 28 total instances, categorized by regions: N. Virginia (16), London (7), and Mumbai (5). The main content area features a search bar with the query 'vulnerability.threatIntel.easyExploit:true and securitygroup.inboundRule.ipv4Range:0.0.0.0' and a filter for 'Last 24 Hrs'. Below the search bar, there are three summary cards: '0 Without Agents', '21 With Public IP', and '2 Docker Hosts'. A table titled 'Resource Summary' lists 28 instances, showing columns for EC2 Instance ID, Account ID, Region, Type, State, and First Discovered On. The table lists instances such as 'i-09877e1ab68f05330' (demo-aws-ue1-windows-2016-public-B) and 'i-03c8e8468ca299184' (demo-aws-ew2-windows-2016-public-C).

EC2 INSTANCE ID	ACCOUNT ID	REGION	TYPE	STATE	FIRST DISCOVERED ON
i-09877e1ab68f05330 demo-aws-ue1-windows-2016-public-B	636123215182	N. Virginia	t2.medium	Running	October 13, 2019 4:46 AM
i-03c8e8468ca299184 demo-aws-ew2-windows-2016-public-C	636123215182	London	t2.medium	Running	October 12, 2019 8:44 PM
i-0e8258f50a903cc4f demo-aws-ew2-ubuntu-16-public-C	636123215182	London	t2.medium	Running	October 12, 2019 8:44 PM
i-0de3c0e9cc738bcf0 demo-aws-ue1-ubuntu-16-public-B-2	636123215182	N. Virginia	t2.micro	Running	September 19, 2019 1:02 AM
i-08ad24b40b2eaf29a demo-aws-ew2-windows-2019-public-C	636123215182	London	t2.medium	Running	August 27, 2019 7:48 PM
i-0ab2ff3ca465eef42 demo-aws-ue1-centos-7-private-B	636123215182	N. Virginia	t2.medium	Running	August 27, 2019 7:48 PM
i-06f41ddd375f62144 demo-aws-mumbai-windows-2016-publi...	636123215182	Mumbai	t2.medium	Running	August 26, 2019 7:41 AM
i-0afd7b51095e0db68 demo-aws-ue1-windows-2008-public-B	636123215182	N. Virginia	t2.medium	Running	August 24, 2019 7:31 PM

# Serverless Visibility

Serverless Visibility  
– Inventory support  
for AWS Lambda  
functions

Best practices  
policy for  
identifying  
misconfigurations

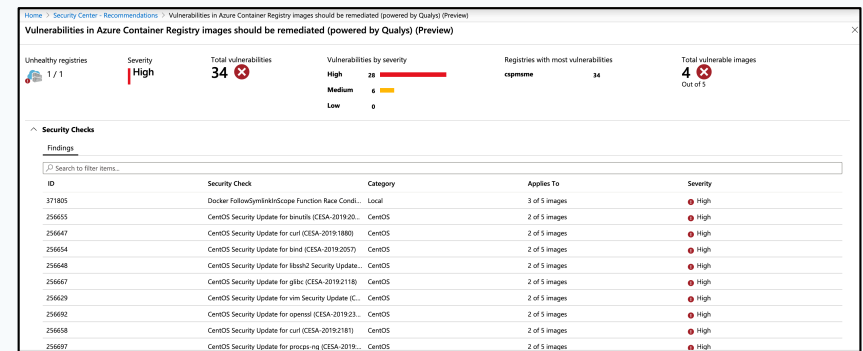




NEW

# Built-in Security with Cloud Providers

- Send findings into Azure, AWS, GCP Security Hubs
- Access & investigate findings from within the Cloud Provider Security console
- Native integration of vulnerability assessment of hosts, containers (MSFT Azure - Powered by Qualys)



Azure Host, Container Scanning (Powered by Qualys)

# Comprehensive Coverage Across Public Clouds



Amazon Web Services



Microsoft Azure



Google Cloud

Google Cloud Platform

- Inventory
- Best practices like CIS benchmarks
- Cloud provider best practices policy benchmarks
- Mandates like PCI, CCM ISS
- Control customization

# Container Security

The background is a solid blue rectangle. It is decorated with a grid of small white dots. The dots are arranged in a pattern that is denser towards the corners, creating a subtle gradient effect. There are three prominent red dots: one in the upper-left corner, one in the lower-right corner, and one in the middle-right area. Each red dot has a soft, circular glow around it.

# Security across the Container Lifecycle

The diagram illustrates the security across the container lifecycle, divided into two main phases: PRE-DEPLOYMENT PHASE and POST-DEPLOYMENT PHASE.

**PRE-DEPLOYMENT PHASE**

- BUILD**: Tools shown include Jenkins, Bamboo, and Ansible.
- SHIP**: Tools shown include Docker and Kubernetes.

**POST-DEPLOYMENT PHASE**

- RUN**: Tools shown include Kubernetes and Docker.
- HOST**: Tools shown include various operating systems (Ubuntu, CentOS, Red Hat) and cloud providers (AWS, Azure, GCP).

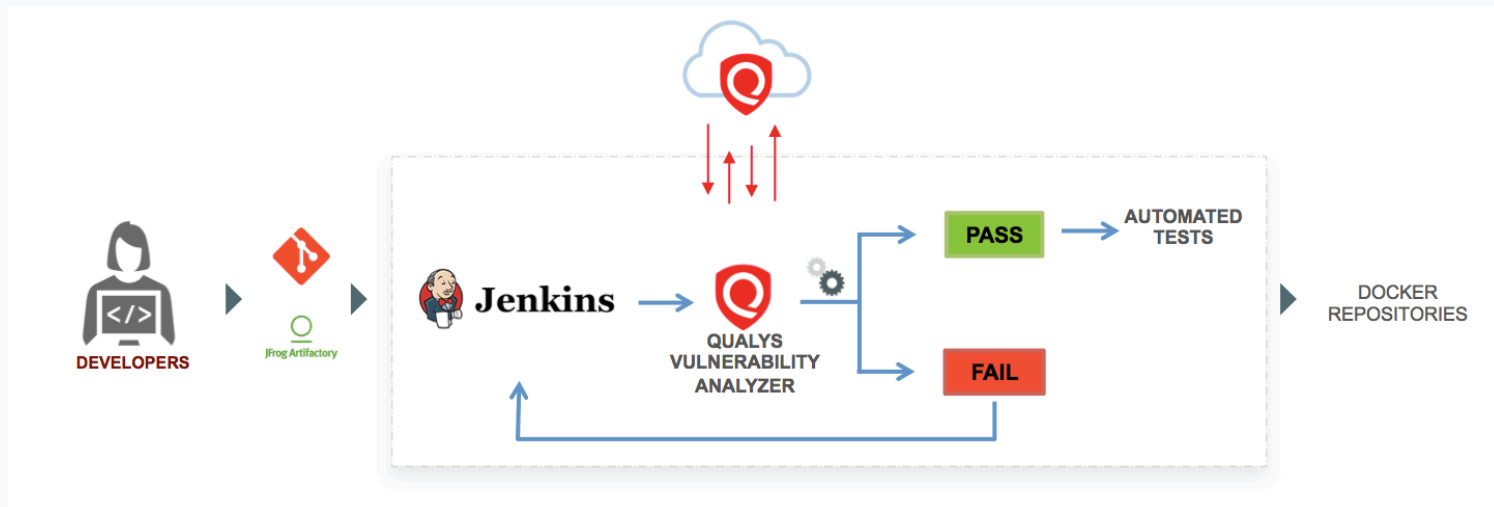
**Security Sensors and Agents**

- Container Sensor**: Associated with the BUILD and SHIP stages.
- CRS and Container Sensor**: Associated with the RUN stage.
- Cloud Agent and/or Scanner Appliances**: Associated with the HOST stage.

Qualys logo is present in the bottom right corner.



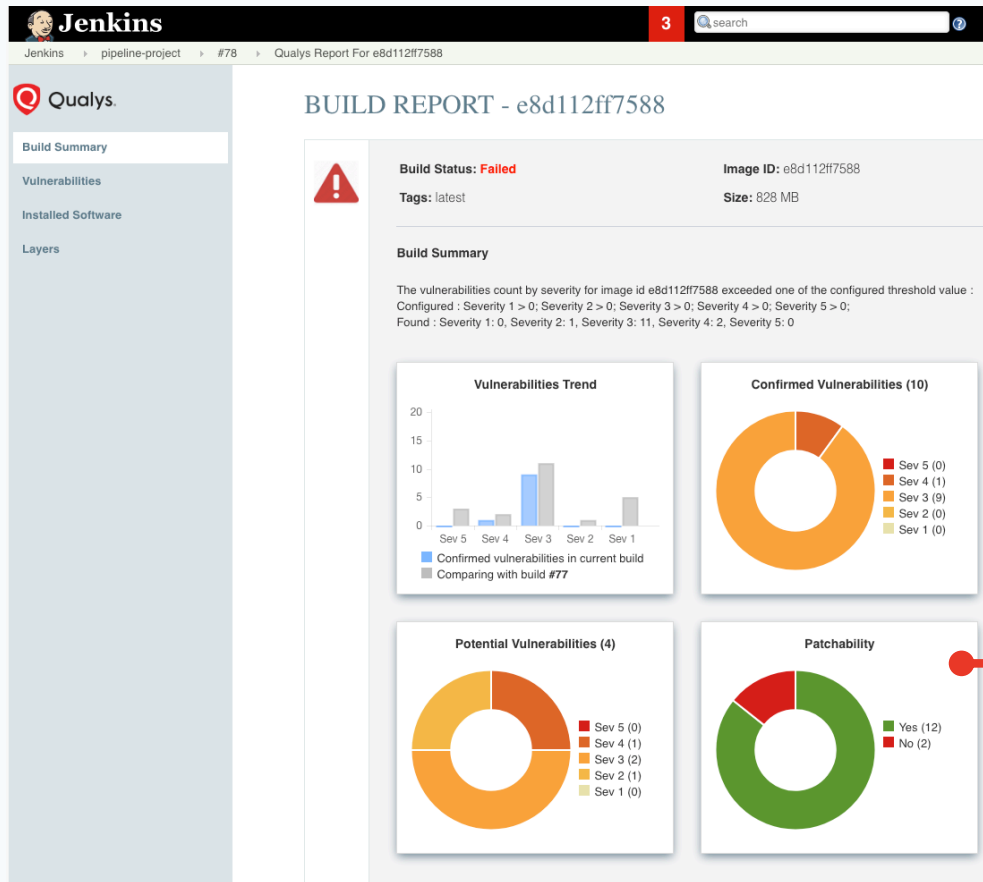
# Scanning Containers in CI/CD



1. DevOps friendly container scanning using a plug-in
2. Actionable, detailed, high-accuracy vulnerability info for DevOps



# Actionable Vulnerability Information for DevOps



Qualys Report For e8d112ff7588 [ENA](#)

## INSTALLED SOFTWARE

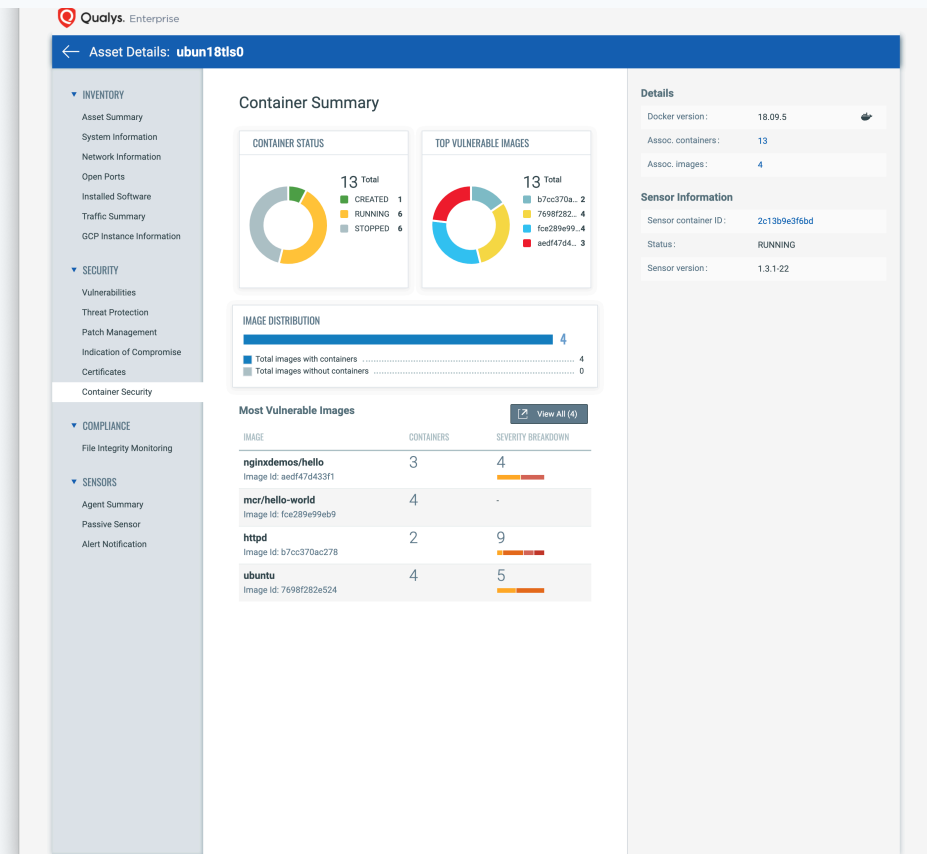
Show 10 entries Search: QID=176259

Name	Installed Version	Fixed In Version
libmagickwand-dev	▲ 8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
libmagickwand-6-headers	▲ 8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
libmagickcore-dev	▲ 8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
libmagickcore-6-headers	▲ 8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
imagemagick-6.q16	▲ 8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4

NEW

# Visibility into Container Infrastructure

- Free inventory for all your container infrastructure
- Visibility into containers via Scanner, Cloud Agent, Container Sensor
- Tracking DockerHub official images
- Upgrade for security across DevOps pipeline

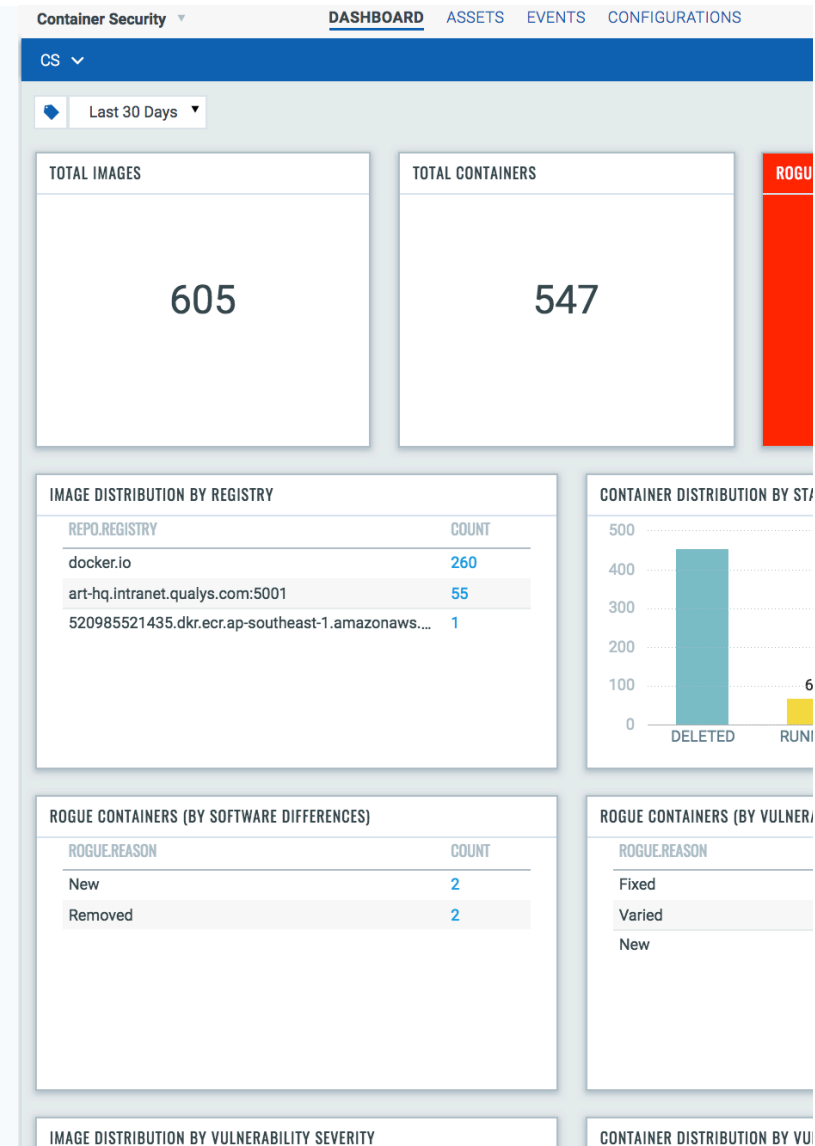


# Deeper Visibility Into Containers

Inventory & security posture widgets

- Count of images, containers
- Containers by state
- Vulnerable images

Personalize and add custom widgets



# Correlating with vulnerability data

Search based on all attributes

Preset quick search filters - Identify images by application labels

68 Total Images

Labels

- NGINX Docker M... 3
- Http://Www.Stind... 1
- GPLV2 1
- /Dockerfile 1
- Git 1
- CentOS Base Ima... 1
- Opsxcq@Strm.Sh 1
- Bad-Dockerfile 1
- CentOS 1
- Reference Docke... 1
- Https://Github.C... 1
- Show less

Registry

- Docker.io 68
- Art-Hq.Intranet.Q... 1

Vulnerabilities

- Severity 5 68
- Severity 4 65
- Severity 3 59

Assets

Images Containers

vulnerabilities.severity:"Severity 5" and repo.registry:"docker.io"

1 - 50 of 68

REGISTRY	REPOSITORY	CREATED ON	TAGS	CONTAINERS	VULNERABILITIES
docker.io	elasticsearch Image Id: 7b3c18d8f363	Feb 06, 2018	latest	0 On Hosts: 1	2
docker.io	redis Image Id: de560ba5403e	Feb 06, 2018	latest	1 On Hosts: 1	3
docker.io	kibana Image Id: 9ef680b9e227	Feb 06, 2018	latest	0 On Hosts: 1	3
docker.io	node Image Id: a606309537c6	Feb 01, 2018	latest	0 On Hosts: 1	3
docker.io	httpd Image Id: 2e202f453940	Jan 26, 2018	latest	1 On Hosts: 1	3
docker.io	cassandra Image Id: e25e005ebec1	Jan 23, 2018	latest	0 On Hosts: 1	4
docker.io	solr Image Id: 0ee0d104030e	Jan 19, 2018	latest	0 On Hosts: 2	14
docker.io	tomcat Image Id: 66bbd06c8cd	Jan 18, 2018	latest	0 On Hosts: 1	13
docker.io	kibana Image Id: 6ded4c70c32d	Jan 17, 2018	latest	0 On Hosts: 1	10

- Image info
- Registry info
- Containers for this image
- Vulnerability posture?
- Easy drill down for complete inventory

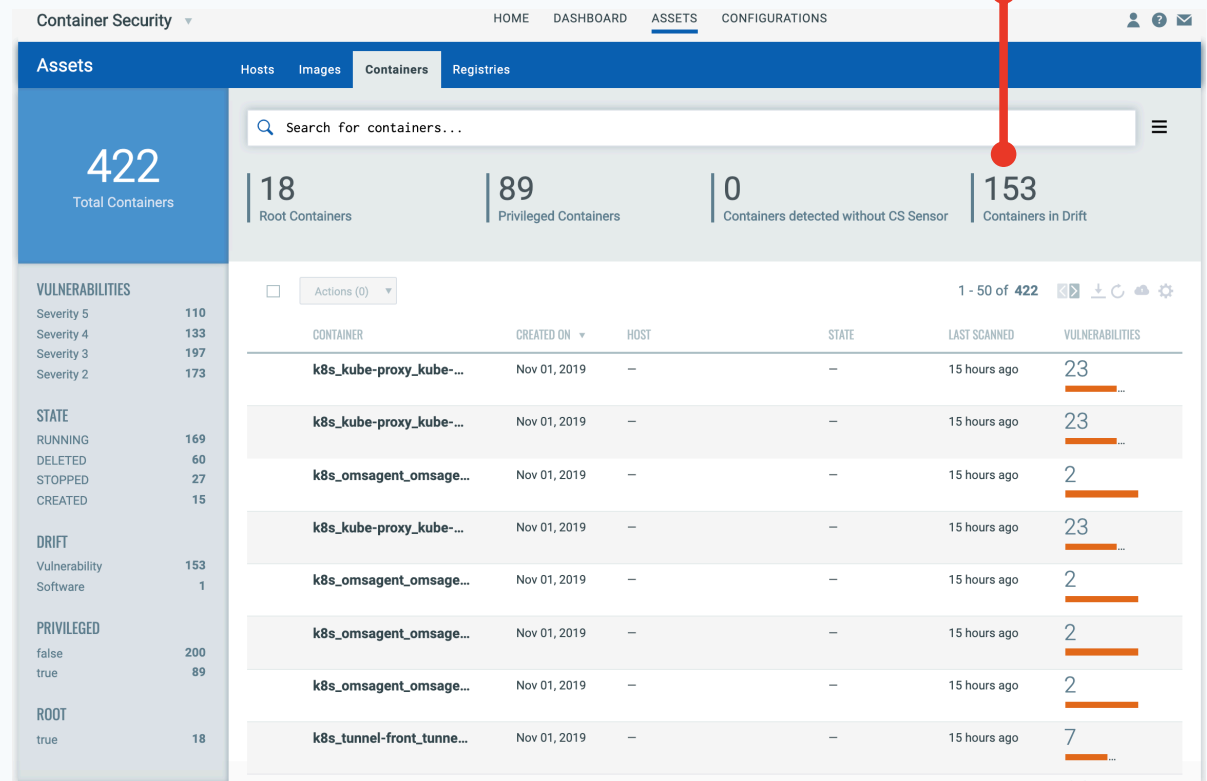
Qualys

# Detecting Runtime Drift

Identify potential breaches in containers

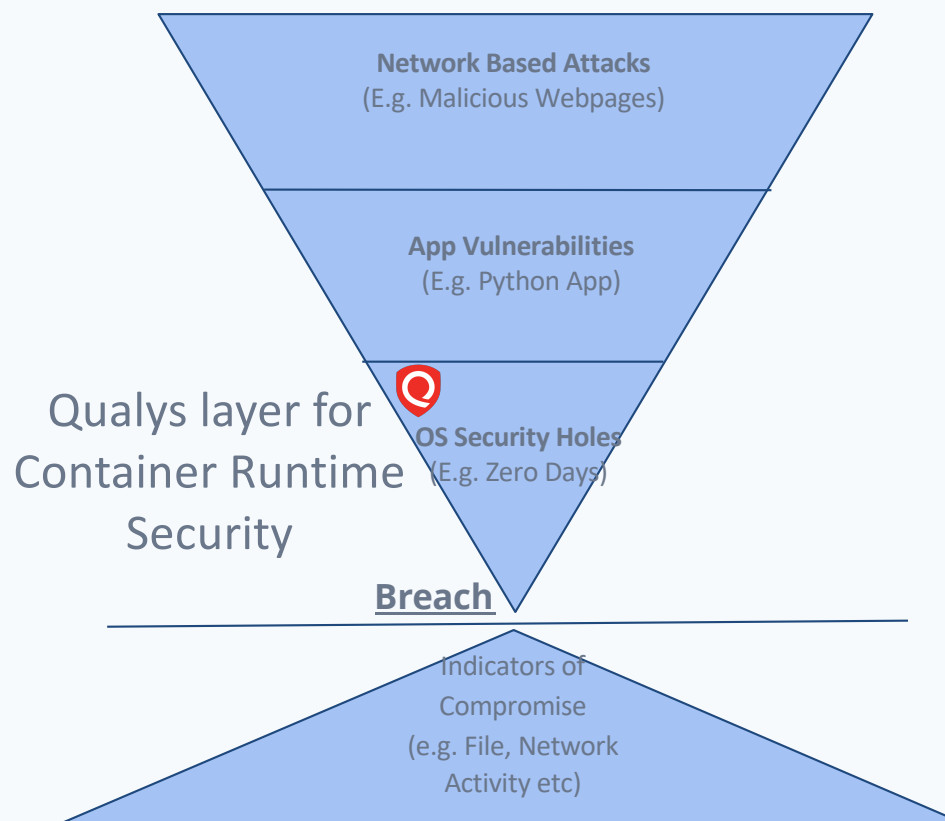
“Drift” Containers, differ from their parent Images by vulnerability, software package composition, behavior, etc

Detect Containers breaking off from “immutable” behavior





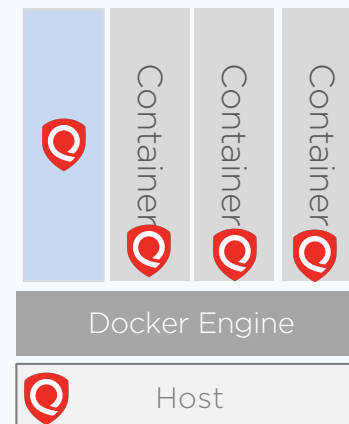
# Protecting Containers at Runtime



NEW

# Protect Against Attacks with Container Runtime Security

- Integrated into Qualys Platform
- Function level firewall for containers
- Granular security policies to control file, network, process behavior
- Built-in policies from Qualys Threat Research



← View Details: e910f86a4411

View Mode

Summary

Container Details

Runtime Analytics

RunTime Profile

Network

Services/Users

Installed Software

Associations

Vulnerabilities

Filter by: All

1 - 50 of 63

LOG	PROCESS	PROCESS ID	CALL	ARGUMENTS	ACCESS	TIME
Behavior log	/sbin/init	1	3	/lib/x86_64-linux-gnu/libselin	Allowed	November 5, 2019 04:26:26AM
Behavior log	/sbin/init	1	0	/lib/x86_64-linux-gnu/libpcre	Allowed	November 5, 2019 04:26:26AM
Behavior log	/sbin/init	1	2	/lib/x86_64-linux-gnu/libblkid	Allowed	November 5, 2019 04:26:26AM
Behavior log	/sbin/init	1	0	/lib/x86_64-linux-gnu/libblkid	Allowed	November 5, 2019 04:26:26AM
Behavior log	/sbin/init	1	3	/lib/x86_64-linux-gnu/libcap	Allowed	November 5, 2019 04:26:26AM
Behavior log	/sbin/init	1	5	/lib/x86_64-linux-gnu/librt-2:	Allowed	November 5, 2019 04:26:26AM

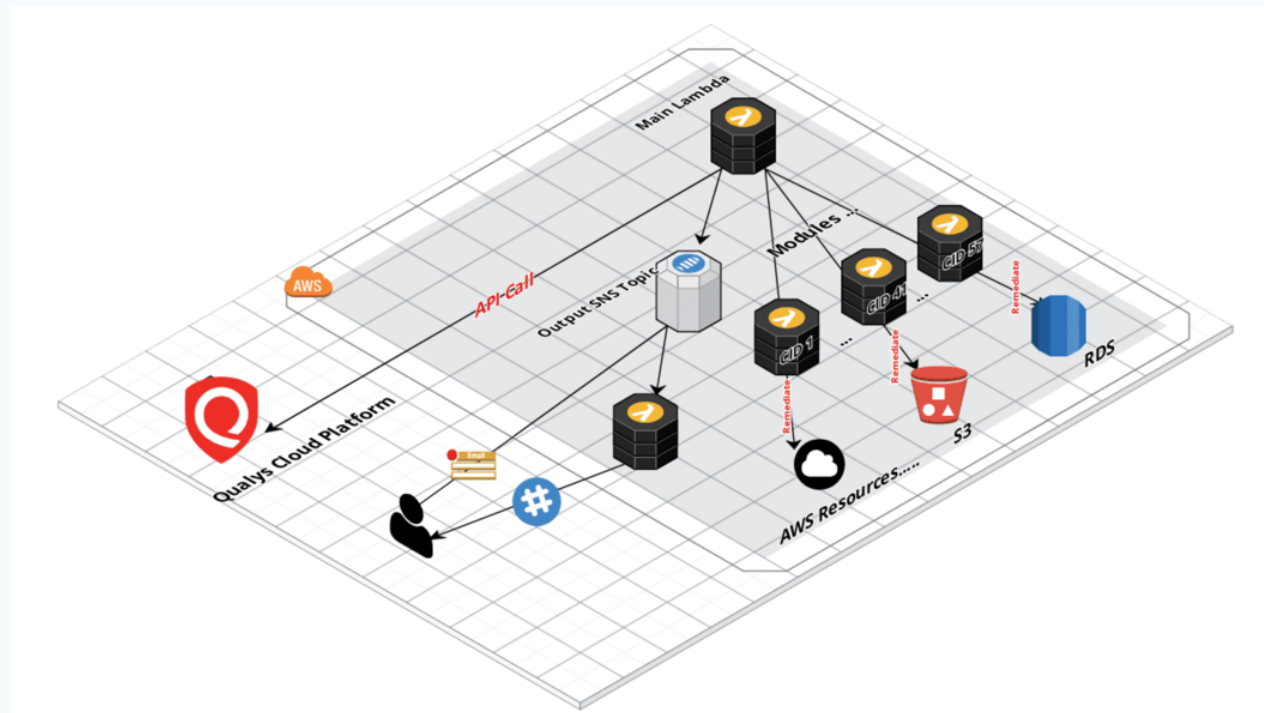
The background is a solid blue color with a pattern of small white dots arranged in a grid. Three red circular highlights are placed on the grid: one in the upper right, one in the lower left, and one in the middle left.

# DEMO

# The Road Ahead



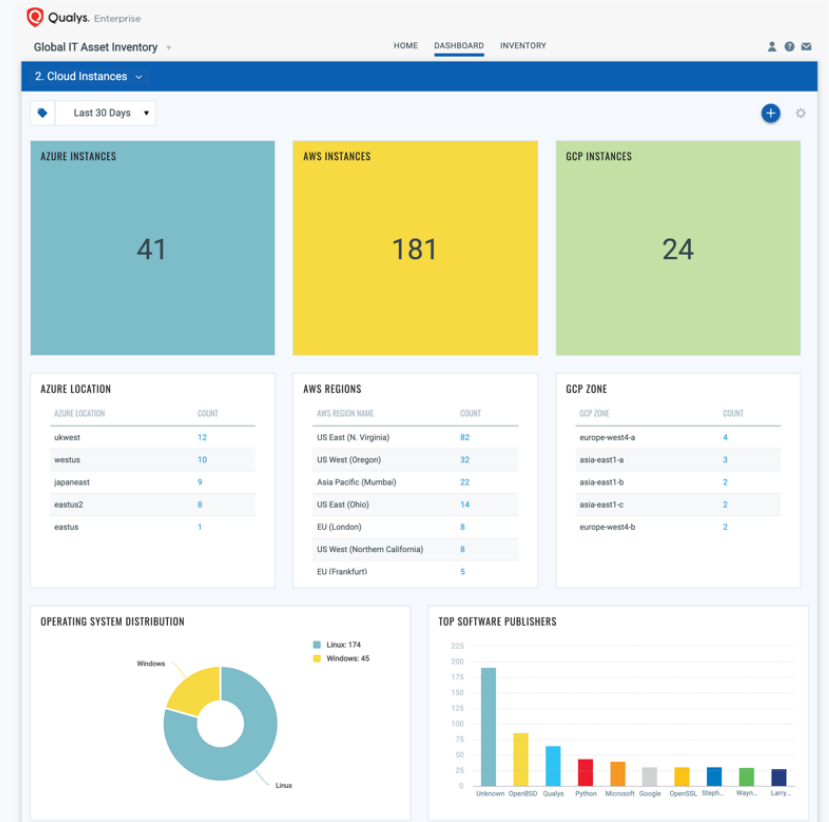
# Moving Towards Automated Remediation



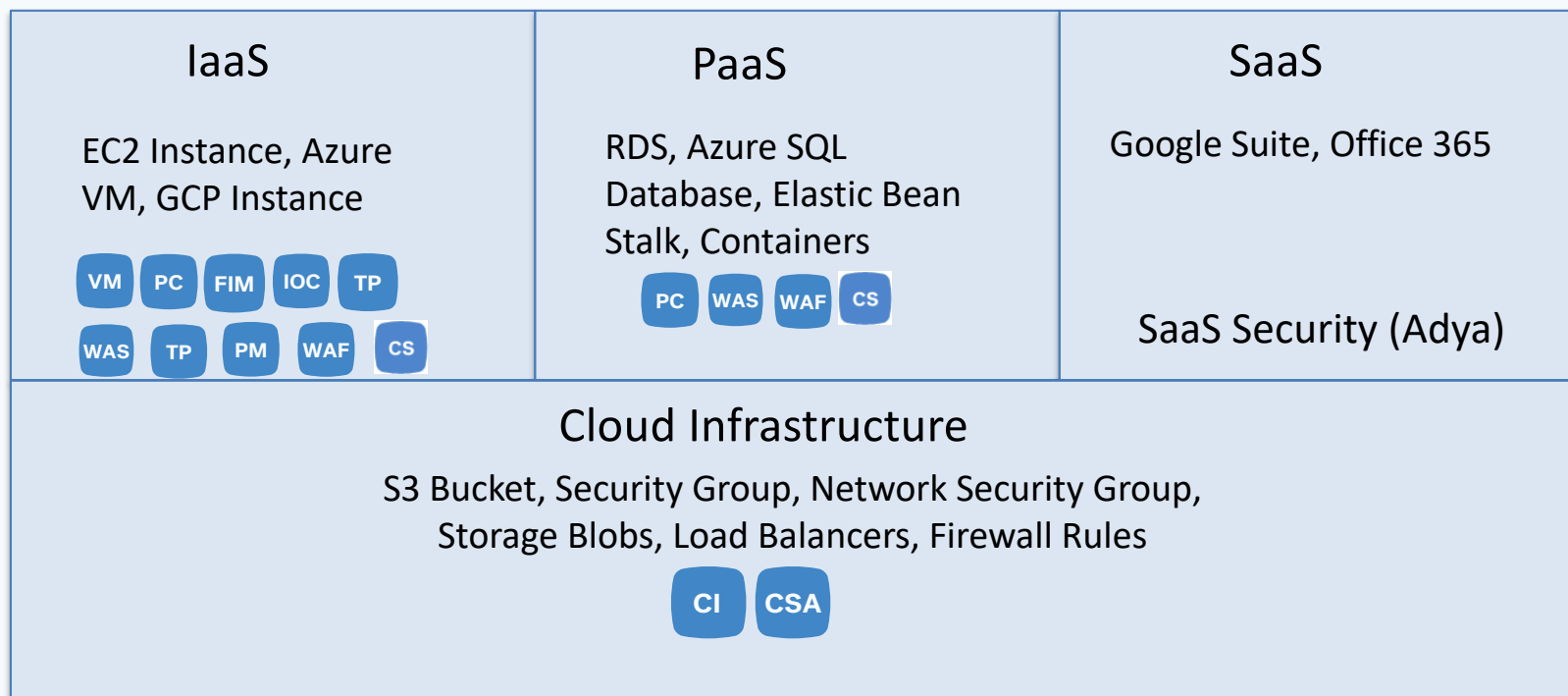


# Towards Seamless Visibility

- Across application stack (Hosts, Kubernetes Pods, Containers, Serverless)
- Correlate cloud inventory data with containers



# Qualys Cloud Security Coverage



# Qualys GitHub for DevOps

- Automation scripts for sensors
- Best practice process automation
- Open source community around Qualys ecosystem

<https://github.com/qualys>







QUALYS SECURITY CONFERENCE 2019

# Thank You

Badri Raghunathan  
[braghunathan@qualys.com](mailto:braghunathan@qualys.com)